NIST
National Institute of Standards and Technology

pseudo-random number generator

(algorithm)

Definition: A *deterministic algorithm* to generate a sequence of numbers with little or no discernible pattern in the numbers, except for broad statistical properties.

Also known as PRNG.

Specialization (... is a kind of me.)
linear congruential generator.

See also *randomized algorithm*.

Note: Any computer program is likely to generate pseudo-random numbers, not actually random numbers. This is important when, say, simulations are sensitive to subtle patterns in the "random" numbers used. Hardware-based random number generators are built from parts with naturally random events, such as noise in a diode.

A generator may be "seeded", or initialized, with a random event, such as the current time in milliseconds, to give different sequences every time it is used.

*Do **NOT** use typical "random" number generators for security or cryptographic purposes. Random Numbers from David Wheeler's Secure Programming for Linux and Unix HOWTO, Section 11.3, gives suggestions and guidelines.*

Author: PEB

Implementation

(C++, C, and Fortran). Herbert Glarner's Mersenne Twister MT 19937 (Linoleum). GAMS (C). Using C libraries to get random numbers in a certain range (C) is C FAQ question 13.16.

More information

Random Number Generation and Testing with links to reports, standard tests, and on-going research. ent: a program to test the randomness of bytes in a file. Karl Entacher's thorough review and comparison of A collection of selected pseudorandom number generators with linear structures.

Go to the Dictionary of Algorithms and Data Structures home page.

If you have suggestions, corrections, or comments, please get in touch with Paul E. Black.

Entry modified 21 May 2007.
HTML page formatted Mon May 21 08:45:03 2007.

Cite this as:
Paul E. Black, "pseudo-random number generator", in *Dictionary of Algorithms and Data Structures* [online], Paul E. Black, ed., U.S. National Institute of Standards and Technology. 21 May 2007. (accessed TODAY) Available from: http://www.nist.gov/dads/HTML/pseudorandomNumberGen.html